

FILED IN CHAMBERS  
U.S.D.C. - Rome

DEC 1 2017

(USAO GAN 6/10) Search Warrant

**United States District Court**  
NORTHERN DISTRICT OF GEORGIA

JAMES N. HATTEN, Clerk  
*Ram Bull*  
Deputy Clerk

In the Matter of the Search of

280 Haven Drive  
Ringgold, Georgia 30736

**APPLICATION AND  
AFFIDAVIT FOR  
SEARCH WARRANT**  
Case number: 4:17-MC-25

I, Shawn M. Owens, being duly sworn depose and say:

I am a Special Agent of the Bureau of Immigration & Customs Enforcement (ICE) and have reason to believe that on the property described as:

280 Haven Drive  
Ringgold, Georgia 30736,  
as more fully described in Attachment A

in the Northern District of Georgia there is now concealed certain property, certain information, and certain data, namely,

computers, computer peripherals, electronic media storage devices, and other items more particularly described in Attachment B,

which constitutes evidence of a crime, contraband, fruits of crime, or items illegally possessed, and property designed for use, intended for use, or used in committing a crime, concerning violations of Title 18, United States Code, Section(s) 2252(a)(4)(B). The facts to support a finding of Probable Cause are as follows:

SEE ATTACHED AFFIDAVIT

Continued on attached sheet made a part hereof.

Sworn to before me, and subscribed in my presence

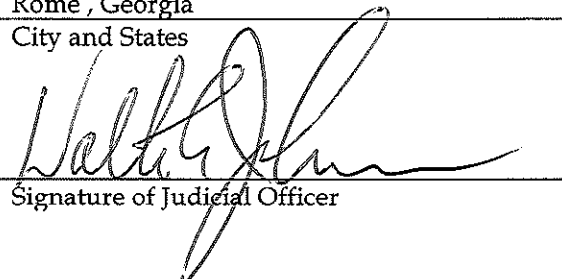
December 1, 2017  
Date

WALTER E. JOHNSON  
UNITED STATES MAGISTRATE JUDGE  
Name and Title of Judicial Officer  
AUSA Paul R. Jones



\_\_\_\_\_  
Signature of Affiant  
Shawn M. Owens

Rome, Georgia  
City and States

  
\_\_\_\_\_  
Signature of Judicial Officer

**AFFIDAVIT**

I, Shawn M. Owens, Special Agent with Homeland Security Investigations (HSI), being duly sworn under oath, hereby state that the following is true and correct to the best of my knowledge and belief:

**INTRODUCTION**

1. I have been a Special Agent with the Department of Homeland Security (DHS) Homeland Security Investigations (HSI) for approximately seven years. Prior to serving as a Special Agent, I served as an Immigration Enforcement Agent with DHS, Immigration and Customs Enforcement, Enforcement and Removal Operations and as a Border Patrol Agent with DHS-United States Customs and Border Protection, Office of Border Patrol. Over the past eleven years, I have led, conducted and/or participated in criminal investigations of matters and offenses such as child exploitation, identity theft, immigration violations, narcotics trafficking, human trafficking and human smuggling.

2. As a Special Agent, I am responsible for enforcing federal criminal statutes, including statutes criminalizing the sexual exploitation of children pursuant to Title 18, United States Code, Sections 2252 and 2252A. I received training and have experience relating to federal criminal procedures, federal statutes, and DHS regulations. I have received training and instruction in the investigation of child pornography offenses and have had the opportunity to participate in investigations relating to the sexual exploitation of children. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as digital images, videotapes, video file and printed images).

3. This affidavit is submitted in support of an application for a search warrant for the property, to include out-buildings and/or separate structures, located at 280 Haven Drive Ringgold, GA 30736 (the Subject Premises), for computer(s) and other related devices and media located therein, as stated in Attachment B, for evidence of violations of Title 18, United States Code, Section 2252(a)(4)(B) that prohibits the possession of visual depictions of minors engaged in sexually explicit conduct and accessing with intent to view such visual depictions. The Subject Premises is more fully described in Attachment A.

4. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(4)(B) are presently located at the Subject Premises. The information contained herein is based on my own investigation, my training and experience, and information provided to me by other law enforcement officers.

#### **BACKGROUND REGARDING SEIZURE OF COMPUTERS**

5. This affidavit is made in support of authorization to search and seize records, computers, and electronic storage media that might be found at the Subject Premises. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

6. For example, I know that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current

state, including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks, tape and/or CD-ROM and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data, and its corresponding evidentiary value, is lost when a computer is powered-off and unplugged.

7. Based on my training and experience, I know that, wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates that files were created and the sequence in which they were created.

8. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

9. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes how the computers were used, the purpose of their use, who used them, and when they were used.

10. In cases like this one, where the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any application software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the

entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment.

11. In cases of this sort, the computer and its storage devices, the mouse, the monitor, keyboard, printer, modem and other system components are also used to operate the computer to commit offenses involving the sexual exploitation of minors. Devices such as modems can contain information about dates, frequency, and computer(s) used to access the internet. The monitor, keyboard, and mouse may also have fingerprints on them indicating the user of the computer and its components.

12. Similarly, files related to the sexual exploitation of children found on computers and other digital communications devices are usually obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants showing the identity of the person engaging in the conduct as well as the method of location or creation of the images, search terms used, and exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

13. "User attribution" evidence can also be found on a computer and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with

the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. I know from training and experience that persons trading, receiving, transporting, distributing or possessing images involving the sexual exploitation of children or those interested in the firsthand sexual exploitation of children often communicate with others through correspondence or other documents which could tend to identify the origin and possessor of the images as well as provide evidence of a person's interest in child pornography or child sexual exploitation.

14. I know from my training and experience that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same Internet Protocol ("IP") address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.

15. Searching computers for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. Or, a person engaged in criminal activity will attempt to conceal evidence of the activity by "hiding" files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of the premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of these premises for the things described in

this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. It is also possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use techniques that are more thorough.

16. Based upon my knowledge, training and experience, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

- a. The nature of evidence: As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a “booby-trap”), the controlled environment of a laboratory is essential to its complete and accurate analysis.



- b. The volume of evidence: Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence by storing it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.
- c. Technical requirements: Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- d. Variety of forms of electronic media: Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

#### **BACKGROUND REGARDING THE INTERNET AND CHILD EXPLOITATION**

17. I have been trained in the investigation of crimes involving the sexual exploitation of children. Based on this training and knowledge, and the experience of other law

enforcement personnel involved in this investigation, I know the information in the following paragraphs.

18. Child pornographers can transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made with literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornography.

19. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of one terabyte or more are not uncommon. These drives can store thousands of images and videos at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with video capture capabilities, and save

that image to storage in another country. Once this is done, there is no readily apparent evidence at the “scene of the crime.” Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

20. With Internet access, a computer user can download an image file from the Internet or from another user’s computer to his own computer, so that the image file is stored in his computer. The user can then display the image file on his computer screen, and can choose to save the image on his computer and/or print out a hard copy of the image. Sometimes the only method to recreate the evidence trail of this behavior is with careful laboratory examination of the computer, modem, printer, and other electronic devices.

21. I know from my training and experience that search warrants of residences involved in computer or digitally related criminal activity usually produce items that tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to obtain child pornography, to include credit card bills, telephone bills, correspondence and other identification documents.

22. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. As noted above, even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space for long periods of time before they are overwritten.

### **CLOUD STORAGE**

23. When using “Cloud Storage” or a “Cloud Account” a user saves files or information to a remote database or server using an Internet connection. This is done instead of storing information to the user’s local computer hard drive or other local storage. Similar to programs like Dropbox, links can be created from within a cloud account to share files with other users.

### **BACKGROUND OF INVESTIGATION**

24. On November 09, 2017, HSI Dalton, GA, received a lead from the HSI Cyber Crimes Center (C3) Child Exploitation Investigations Unit (CEIU) concerning the German Federal Criminal Police Office (Child Porn Unit S043) through Interpol relating to U.S. IP addresses<sup>1</sup> identified in S043’s Operation Cloud. The IP address of a user who streamed child sexual abuse material related to this investigation was identified as originating in the Ringgold, GA, area.

25. The S043 received information from the German Internet Service Provider “1&1 Internet SE” that an unknown user with the email address “dsfl1811@web.de” stored child sexual abuse material in the folder “pt” of the user’s cloud storage. Users could access this material using the link:

**[https://c.web.de/@428642995647027013lNEpAijQy2W0sLT4vRS\\_A](https://c.web.de/@428642995647027013lNEpAijQy2W0sLT4vRS_A)**

---

<sup>1</sup> The Internet Protocol address, or IP address, is a unique set of numbers that a computing device, such as personal computers and smart phones, use to identify itself and communicate with other devices on a network. The IP address allows investigators to identify the location of a computer connected to the internet at a certain time.

26. German Internet Service Provider “1&1 Internet” provided the IP addresses with corresponding date/time stamps for users who streamed the child sexual abuse material videos online through their Internet browsers between July 9 and August 10, 2017.

27. German law enforcement provided a spreadsheet titled “IPaddresses\_countries.xls” with the corresponding IP address, the Internet Service Provider, and associated country. German law enforcement provided a spreadsheet titled “filtered-requests.csv” which lists the accessed videos by filename and the corresponding IP addresses with date/time stamps. German law enforcement also provided the child sexual abuse material videos, which were posted to the “pt” folder in the cloud storage link listed above.

28. As part of the above referenced activity, IP address 64.18.112.185 was identified as streaming at least two videos containing child sexual abuse material from the target link. C3 CEIU established that Internet Service Provider “RTC (Ringgold Telephone Company) Internet” is related to this IP address.

29. C3 CEIU sent legal process on the identified U.S.-based IP addresses, including to “RTC Internet” for IP address 64.18.112.185, and generated spreadsheets and folders of the child sexual abuse material streamed using each of the U.S. IP addresses.

30. On November 08, 2017, RTC (Ringgold Telephone Company) Internet, located in Ringgold, GA, responded to the legal process submitted for IP address 64.18.112.185.

31. On November 15, 2017, I reviewed the response from RTC Internet concerning IP Address 64.18.112.185. Upon reviewing the response, I determined that IP address 64.18.112.185 has the following account information assigned to it:

**Service Activation Date:** March, 2011  
**Account Number:** 00024452-6

**Account Owner:** Eddie D. POOLE, DOB: XX/XX/1959, Cell: XXX-XXX-2212

**Secondary Account Owner:** Patti POOLE, DOB: XX/XX/1960

**Account Service Address:** 280 Haven Drive Ringgold, GA 30736

32. The response from RTC Internet also disclosed that the last payment made for this account covered the October, 2017 billing cycle. This payment was made using an online bill pay through a Regions Bank, NA account listed to Eddie POOLE.

33. On November 15, 2017, HSI Dalton, I conducted open source and Law Enforcement database checks related to 280 Haven Drive Ringgold, GA 30736 (Subject Premises). SA Owens noted three listed occupants of the Target Address:

- a. Eddie (Edward) Daniel POOLE, DOB: XX/XX/1959, SSN: XXX-XX-0172
- b. Patricia (Edwards) POOLE; DOB: XX/XX/1960, SSN: XXX-XX-0878
- c. Eric M. EDWARDS, DOB: XX/XX/1989, SSN: XXX-XX-0172

34. The Subject Premises is listed as being "Owner Occupied" by Eddie POOLE and Patricia (Edwards) POOLE. Both of these subjects currently have multiple vehicles registered to this address.

35. Eric EDWARDS currently shows utility hook-ups in Edward's name at the Subject Premises. EDWARDS also has at least one vehicle that was registered to the Subject Premises in his name during 2017.

36. On the same day, SA Owens conducted Law Enforcement Database checks on Eddie POOLE (XX/XX/1959) and Eric EDWARDS (XX/XX/1989). Database returns indicate that POOLE maintains a current Georgia driver's license and that license indicates POOLE's current address is 280 Haven Drive Ringgold, GA 30736 (Subject Premises). Database returns

indicate that EDWARDS maintains a current Georgia driver's license and that license indicates EDWARDS' current address is 280 Haven Drive Ringgold, GA 30736 (Subject Premises).

37. On November 15, 2017, HSI Dalton, I received the digital evidence associated to this case. I was able to extract and analyze this evidence, and upon examination I noted a folder named "pt", as it was named on the cloud storage account. Located inside of the "pt" folder were two digital video files. Each of these video files depicted a prepubescent child being sexual abused:

- a. **6yo latina fucked both ways.mp4** – This video file opens to the image of a very young prepubescent female child lying on the bed. The child is naked from the waist down with her legs spread. The child's vagina is clearly viewable in the frame. An adult male then begins engaging in sexual intercourse with the child as she is lying on her back. The adult male then rolls the child over and engages in sexual intercourse with the child while she is lying on her stomach. The adult male removes himself from the child and the video shuts off.
- b. **Hot Latin doggiefucking.mp4** – This video file opens to the image of prepubescent child. The video shows the child's naked rear-end as an adult male is engaging in sexual intercourse with the child from behind. The adult male continues to engage in this activity with the child until he ejaculates on the child's rear-end. The video then shuts off.

38. Both of the above referenced files were streamed by IP address 64.18.112.185 in August 2017 while the IP address was associated to the residence at 280 Haven Drive Ringgold, GA 30736 (Subject Premises).

39. On November 13, 2107, I conducted surveillance in the area of the Subject Premises. SA Owens discovered that the Subject Premises is located at the end of a cul-de-sac and the Subject Premises is situated behind another house. The Subject Premises is not viewable from the street, and SA Owens was not able to get close enough to the Subject Premises to scan for wireless networks.

**INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN AND RECEIVE  
AND/OR DISTRIBUTE CHILD PORNOGRAPHY**

40. Based on my previous training and participation in child pornography and related investigations, I have learned that individuals who possess, receive, distribute or access with intent to view child pornography have a sexual interest in children and in images of children, and downloading images and videos of child pornography. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

- a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.
- b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, videotapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child



pornography but which nonetheless fuel their deviant sexual fantasies involving children. Individuals who collect child pornography often store it on multiple devices to be collected, viewed or traded at a later date. For example, devices such as a thumb drive and/or portable hard drive are used to transfer a downloaded image from one device (e.g., computer) to another device (e.g., tablet).

- c. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collections of illicit materials from discovery, theft, and damage. They almost always maintain their collections in the privacy and security of their homes or another secure location.
- d. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, email, email groups, bulletin boards, Internet relay chat, newsgroups, instant messaging, and other similar vehicles.
- e. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own

feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

- f. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

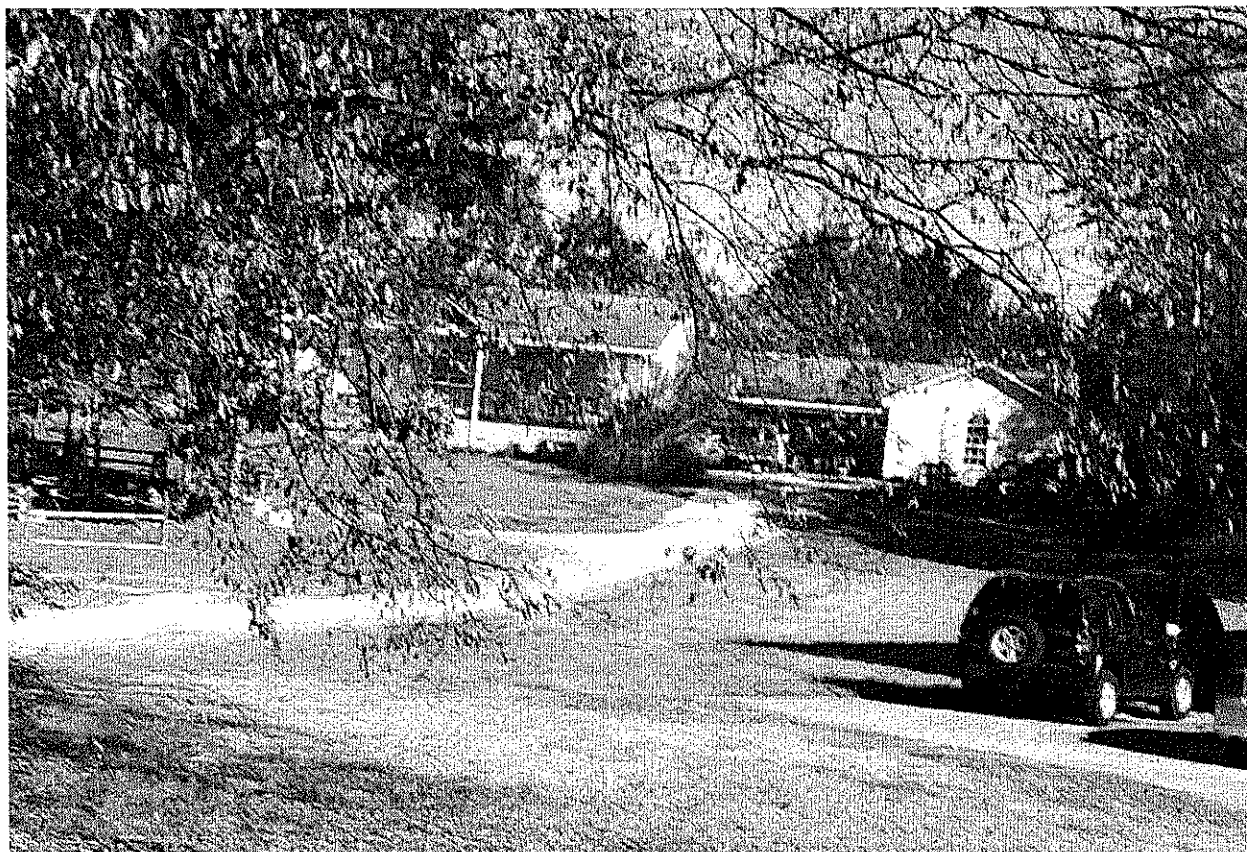
### **CONCLUSION**

41. Based on the investigation described above, there is probable cause to believe that at the property located at 280 Haven Drive Ringgold, GA 30736, described in more detail in Attachment A, will be found evidence, fruits, and instrumentalities of a violation or violations of Title 18, United States Code, Section 2252(a)(4)(B) (the possession of visual depictions of minors engaged in sexually explicit conduct, and accessing with intent to view such depictions), described in greater detail in Attachment B. I, therefore, respectfully request that the attached warrant be issued authorizing the seizure and search of the items listed in Attachment B.

**ATTACHMENT A**

**DESCRIPTION OF LOCATION TO BE SEARCHED**

The Subject Premises is located at 280 Haven Drive, Ringgold, GA 30736. This residence is located at the end of the cul-de-sac on Haven Drive. One enters the near the mailbox numbered 280. When the driveway splits, one stays to the left and follows the driveway between two brick columns. The column on the left bears "280" in gold numbers. The house is a white single-family residence with a separate garage/living space connected to the house by a roof over the carport. The request to search includes all buildings and vehicles located on the property.



**ATTACHMENT B**

**DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED**

The following items, located at 280 Haven Drive Ringgold, Georgia 30736, to include any and all outbuildings at that location that constitute contraband or evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Section 2252:

1. Images or visual depictions of minors engaged in sexually explicit conduct.
2. Records and information containing child erotica, including texts, images and visual depictions of child erotica.
3. Any and all information, notes, software, documents, records, or correspondence, in any format and medium pertaining to violations of Title 18, United States Code, Section 2252.
4. Any and all information, notes, documents, records, or correspondence, in any format or medium concerning communications about child pornography or sexual activity with or sexual interest in children.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of committing violations of Title 18, United States Code, Section 2252.
6. Any and all information, notes, documents, records, or correspondence, in any format or medium concerning membership in online groups, clubs, or services that provide or make accessible child pornography.
7. Any and all cameras, film, videotapes or other photographic equipment that constitute contraband or evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Section 2252.
8. Any and all information, records, documents, invoices and materials, in any format or medium that concern any accounts with an Internet Service Provider.
9. Any and all information, records, documents, invoices and materials, in any format or medium that concern email accounts, online storage, or other remote computer storage.
10. Any and all information, documents, records, or correspondence, in any format or medium pertaining to occupancy or ownership of the premises and use or ownership of computer equipment found in the premises.
11. Credit cards, credit card information, including, but not limited to, bills and payment records pertaining to violations of Title 18, United States Code, Section 2252.

12. Computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, digital storage media, flash drives, external hard drives, compact discs, digital video discs, any physical object upon which computer data can be recorded, gaming devices, digital communications devices, tablets, cellular telephones, cameras, videotapes, video recording devices, video recording players, video display monitors, digital input and output devices such as keyboards, mice, scanners, printers, monitors, electronic media and network equipment, modems, routers, and external or connected devices used for accessing computer storage media that was used to commit violations or facilitate commissions of violations of Title 18, United States Code, Section 2252.
13. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, COMPUTER) that is called for by this warrant, or that might contain items otherwise called for by this warrant:
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, calendars, browsing history, user profiles, e-mail, e-mail contacts, "chat" or instant messaging logs, photographs, and correspondence;
  - b. evidence of software that may allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
  - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - f. evidence of the times the COMPUTER was used;
  - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
  - h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - i. contextual information necessary to understand the evidence described in this attachment; and
  - j. volatile data necessary to preserve evidence prior to powering-off and unplugging a running computer.



14. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
15. Any and all material that is evidence of the sexual interest in children to include, but not limited to, children’s undergarments, sexual devices pertaining to children and other material related to children that is sexual in nature or used for sexual fantasies.